C. Remarks

1. Status of the Claims

Claims 1-20 are pending in the application. Claims 1-2 stand finally rejected under 35 U.S.C. § 102(b) as being anticipated by European Publication No. EP 0 636 962 A2 ("Chou"). Claims 3-20 stand rejected under 35 U.S.C.§ 103(a) as unpatentable over Chou in view of various other references. Applicants hereby amend claims 1 and 11 and add new claims 21-30.

2. Applicants' Record of Interview Conducted October 31, 2006

The Examiner and Applicants' undersigned attorney participated in a telephonic interview on October 31, 2006, to discuss the pending rejections as set forth in the attached copy of the Applicant Initiated Interview Request Form that Applicants' attorney sent by facsimile to the Examiner on October 26, 2006, using the facsimile number provided at page 19 of the pending Office Action. Applicants' attorney understands that the Examiner had not received the foregoing documents prior to the interview. The Examiner nevertheless agreed to proceed with the interview, for which Applicants are grateful.

The Examiner and Applicants' attorney did not reach agreement as to the propriety of the pending rejections, as discussed further below in Section C.4, but did reach agreement that the cited references do not teach a system as recited in the pending claims in connection with the further limitation that the first key portion is generated independent of information specific to the hardware product in connection with which the software product is provided for use.

3. The Amended And New Claims are Allowable Over The Cited References.

Applicants hereby amend claim 1 to recite "said first key portion is generated independent of said hardware product" and amend claim 11 to recite "generating a first key portion of said first encryption key independent of said hardware product." Support for these

amendments can be found, for example, at page 4, lines 13-16 of the specification, which indicates that (i) a first key (KEY A) can be generated using a random number generator, (ii) a first key portion (one of SPLIT A and TOKEN) can be generated using the first key and a random number generator, and (iii) a second key portion (the other of SPLIT A and TOKEN) can be generated utilizing modulo-2 addition of the first key and the first key portion. Nothing else is needed to generate the first key and first and second key portions. As such, the hardware product in connection with which the software product is to be provided is irrelevant to the generation of the first key and first and second key portions.

Based on the above, Applicants submit that amended claims 1 and 11 distinguish over the cited references and, therefore, are allowable. Because claims 2-10 depend from claim 1 and claims 12-20 depend from claim 11, Applicants submit that each of these claims is allowable as well.

Each of new claims 21-30 depends from either claim 1 or claim 11. As such, these new claims are allowable as well. Support for these new claims can be found, for example, at page 4, lines 13-16, as discussed above.

4. Applicant's Comments On Examiner's Interview Summary And Position On Rejections Of Previously Presented Claims

Applicants respectfully disagree with the Examiner's characterization in the Interview Summary mailed on November 3, 2006 that "Applicant agrees that amendment is necessary to particularly point out the invention wherein said "....the first key portion is generated apart from said hardware product;" (interpreted as generating a first key portion in a separate/second computer from hardware product)." Although Applicants suggested amendments as set forth above and agreed to submit such amendments in order to expedite the prosecution of this application, Applicants did not agree that such amendments are necessary to distinguish over the

cited references. Indeed, Applicants maintained their position that the pending rejection of claim 1 is improper for the following reasons.

The Examiner finally rejected claim 1 as previously presented as anticipated by Chou. Applicants submit that claim 1 as previously presented distinguished over Chou for at least two important reasons. First, claim 1 as previously presented recited using a first encryption key to encrypt a software product and using the same encryption key to decrypt the encrypted software product. Although Chou teaches use of a decryption key K to decrypt an encrypted software product, *see* Chou at col. 4, ll. 19-22 and 45-49, Chou does not teach that decryption key K is the same key used to initially encrypt the software product. Notwithstanding, in paragraph 2 of the Office Action, the Examiner has concluded that Chou's key K, which is used to decrypt the software described therein, is also used to encrypt such software. The Examiner, however, has not pointed to any specific passage of Chou for support. There is none. Chou is silent on the key used for encryption and does not teach that the key used for decryption also is used for encryption. For this reason alone, the pending rejections of claims 1-10 are improper and should be withdrawn.

Second, claim 1 as previously presented recited that Applicants' invention provides a first key portion, a second key portion, and an encrypted initial software product for use in a hardware product, "wherein said first key portion is generated apart from said hardware product," that is, the hardware product for use in connection with which the software product is provided. In contrast, Chou teaches providing an encrypted software product to a user's computer, *i.e.*, a hardware product, along with an unencrypted installation utility that generates a first key portion in the user's computer using information specific to, identifying, and/or generated in or by the user's computer. More particularly, Chou states:

> Referring now to the drawing, the distributed encrypted software program 10 which has been produced and distributed includes an unencrypted installation part or unencrypted separate installation utility. This installation utility, when applied to a user's computer, will extract all the information from the computer to provide a unique factor, e.g., form a computer profile and/or a random factor, e.g., the time of entry measured in second intervals, for example, in one tenth or one hundredth of a second intervals which may be entered in the computer, as shown in block 12 of the drawing. The entry, for example, can be made by pressing a key on the computer or may be done automatically by direction from the installation utility. As shown in block 11, other inputs from the keyboard, magnetic or smart card readers, etc. may be applied to the computer for providing unique and/or random factors which are entered.
>
> The aforesaid file referred to as the installation data file is stored on the computer hard disk. The installation utility reads the installation data file and based on its contents, generates a first key K_1 that is presented to user as shown in the block 14.
>
> The user then calls an 800 number or otherwise communicates with a central processing center which controls the use of the distributed program and provides K_1 to the processing center as shown in block 14 of the drawing.

Chou at col. 3, l. 49 - col. 4, l. 19. The Examiner has interpreted first key K_1 to correspond to the first key portion of the present invention. *See* Office Action at 3, lines 4-5. The computer referred to in the foregoing passage, however, is the same computer (*i.e.*, the hardware product) to which the encrypted software product was provided. As such, Chou generates a first key portion in the hardware product to which the software product is provided. Thus, Chou clearly does not teach providing a first key portion to the user's computer, wherein said first key portion is generated apart from said user's computer. In fact, Chou teaches squarely away from such a limitation. For this additional reason, the pending rejections of claims 1-10 are improper and should be withdrawn.

Applicants note the Examiner's citation in connection with the rejection of claim 1 under 35 U.S.C. § 102 to U.S. Patent No. 6,966,002 ("Torrubia-Saez") as purportedly disclosing a first key portion apart from a hardware product to which a software product was provided. Applicants understand this citation to be an effort to combine references in support of such

rejection. Applicants submit that such combination of references is improper in connection with a rejection of a claim under 35 U.S.C. § 102 because a rejection under that section must be based upon a single reference teaching each and every limitation set forth in the claim at issue.

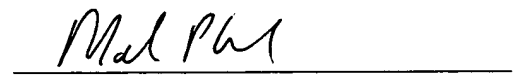
The Examiner finally rejected claim 11 as previously presented as unpatentable over Chou in view of Chan, U.S. Patent No. 5,150,407. Applicants submit that claim 11 as previously presented is patentable over the foregoing combination of references. Claim 11 as previosuly presented explicitly recited a method for providing for the security of encryption keys for encryption and decryption of an initial version of a software product provided to a user of a hardware product, comprising the steps, among others, of encrypting the initial version of said software product with a first encryption key to generate an encrypted initial software product and splitting said first encryption key into first and second key portions by generating a first key portion of said first encryption key apart from said hardware product and utilizing said first key portion and said first encryption key to calculate a second key portion of said first encryption key such that the combination of said first and second key portions form said first encryption key. As discussed above in connection with claim 1, Chou does not teach providing a first key portion to the user's computer, wherein said first key portion is generated apart from said user's computer. Nor does Chan. Chan is directed to a hardware product for storing data. Although Chan discloses separating a key into first and second key portions, Chan does not teach generating said first key portion apart from said hardware product. Indeed, one skilled in the art would understand that both the first and second key portions disclosed by Chan are generated in/by the hardware product on which the data is stored. As such, neither Chou nor Chan nor the combination thereof discloses "generating a first key portion of said first encryption key apart

from said hardware product." For these reasons, the pending rejections of claims 11-20 are improper and should be withdrawn.

5. Conclusion

Based on the above, Applicants respectfully submit that the applicant is in condition for allowance and respectfully request reconsideration thereof.

Respectfully submitted,



Mark P. Vrla
Registration No. 43,973

Dated: November 20, 2006

JENNER & BLOCK LLP
330 North Wabash Avenue
Chicago, IL 60611
Telephone No: (312) 222-9350
Facsimile No: (312) 527-0484

ATTACHMENT A

Chou teaches nothing about the key used for encryption; Chou's generates a first key portion generated in the user's computer, *i.e.*, the hardware product where the software product is to be used; Chou's first key portion is based on information specific to identifying the user's computer; Applicant's invention generates the first key portion apart from the hardware product where the software product is to be used, and such first key portion is independent of characteristics specific to that computer.